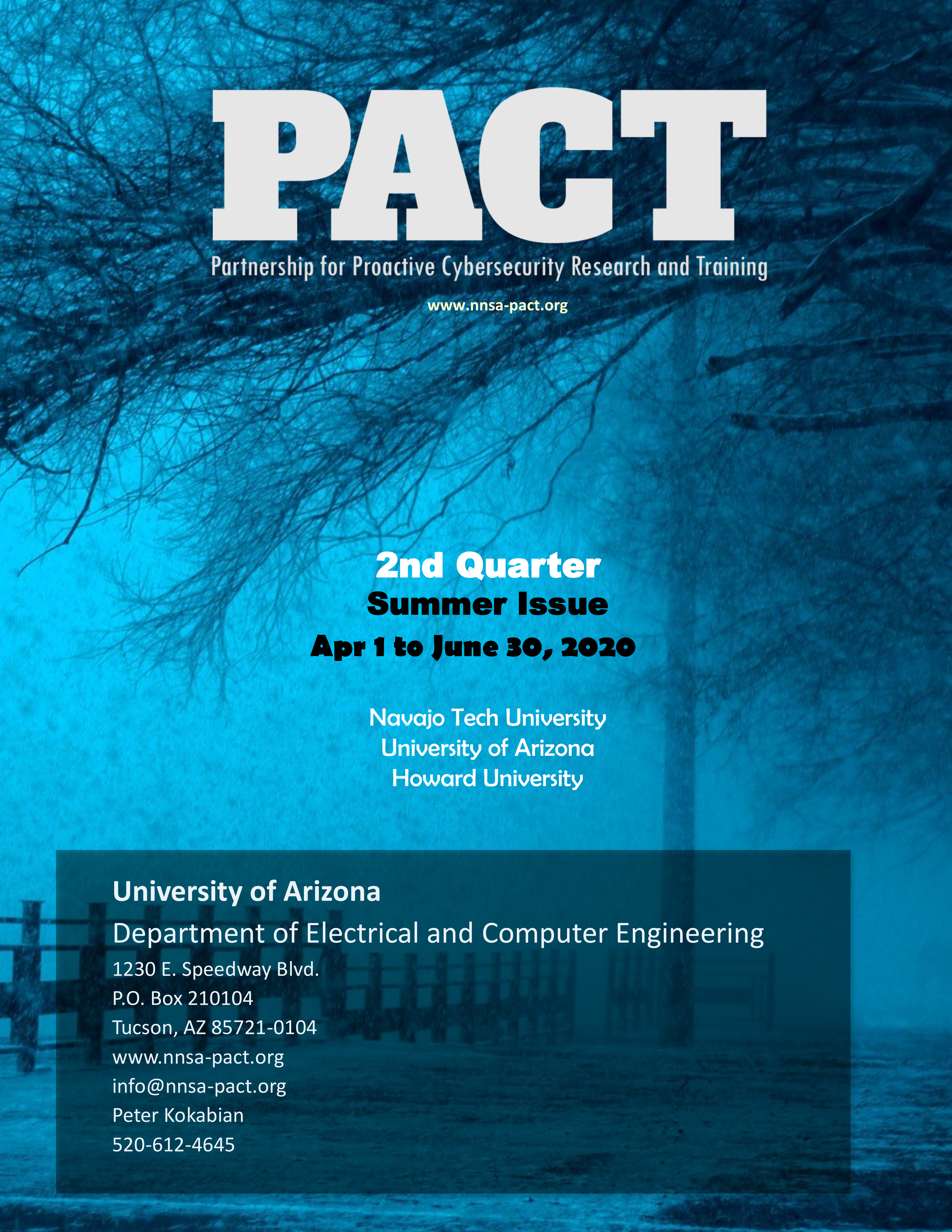


PACT

Partnership for Proactive Cybersecurity Research and Training

www.nnsa-pact.org

2nd Quarter
Summer Issue
Apr 1 to June 30, 2020

Navajo Tech University
University of Arizona
Howard University

University of Arizona
Department of Electrical and Computer Engineering
1230 E. Speedway Blvd.
P.O. Box 210104
Tucson, AZ 85721-0104
www.nnsa-pact.org
info@nnsa-pact.org
Peter Kokabian
520-612-4645

Inside this issue

PACT Newsletter

National Nuclear Security Administration · PACT Partnership for Proactive Cybersecurity Research and Training · U.S. DEPARTMENT OF ENERGY
THE UNIVERSITY OF ARIZONA · HOWARD UNIVERSITY 1867 · Nitsáhákees Nahátá Íína Siihasin NAVAJO TECHNICAL UNIVERSITY ESTABLISHED 1979 · Argonne NATIONAL LABORATORY

Issue (2) nnsa-pact.org Summer 2020

Welcome to Second Issue of PACT Newsletter

Salim Hariri, University of Arizona

It is my pleasure to present to you a new issue of PACT newsletter of Summer 2020. In this issue, we highlight the ongoing research and training activities that were developed and currently used to research and development by students in the cybersecurity, wireless and machine learning sphere For the period of April 1 to June 30, 2020. The partnership will heavily recruit underrepresented minority students to be involved in our research projects, cybersecurity workshops and training and internship programs.

PACT April Workshop

One of the main events of this quarter was the joint workshop with other partner universities. The workshop held on April 24, 2020 through Zoom session.

For the first time under PACT program, online workshop designed to engage, educate, and bring students with cybersecurity background under PACT program together. The primary purpose of our one-day 8-hour workshop was to ensure that students and researchers from all three partner universities share latest research and development activities and bring together graduate students, undergraduate and professors from all computer science majors who were interested in cybersecurity through virtual Zoom platform.

The workshop presented a series of presentations focused on machine learning, cybersecurity, blockchain and wireless security.

Cloud security
Machine Learning
Network and systems security
Wireless Security
Blockchain systems
Intrusion detection systems
Data Forensics

Dr. Tunc New Position

We are delighted to announce the news that one of the our University of Arizona graduates has taken a new faculty position with University of North Texas.

We would like to congratulate Dr. Cihan Tunc in his new position and we wish him a great success and prospering academic endure. Dr. Tunc has been as asset to cybersecurity sphere and academic domain.

April 24 Workshop Presentations

Hololens/Cyber Security Visualization

The Microsoft Hololens is a mixed reality headset consisting of multiple sensors, advanced optics, and holographic processing. It is an excellent way to promote creation and innovation through models and prototypes that can be brought into the real world. What we researched is how we can expand upon utilizing global and local network topologies to be able to visualize and map networks using a barcode-like feature applied to hardware devices. We talked about implementing an identification feature that could leverage mixed reality to map physical devices to the virtual rendering of the network. This allows routers, switches access points, etc. to be mapped, which could allow for mapping while also being paired with tech like Wireshark. By having every physical device mapped in the network, it would be easier to visualize where issues are occurring in a system.

Network-Based Intrusion Detection System in IoT Devices

The main focus of the research opportunity was to investigate how Named Data Networking (NDN) can be used to offer cybersecurity for networked systems with high mobility, dynamic connectivity, better privacy, and low delay. During further research, I came to the understanding that there are challenges in utilizing IP-based IoT solutions. Inherited concerns from the host-based IP addresses are impacting communication performance in the existing and upcoming Internet. Using IP addresses produces a need for additional resolution systems to translate application requests into IP addresses, uses end to end security and supplementary protocols to sustenance mobility. One promising solution to this issue is Named Data Networking. NDN has gained attention because of its simple communication model, scalable naming and lightweight configuration and management operations. NDN treats data as a “1st class citizen” by naming it. This naming system is very human friendly and resembles URLs. NDN is a network service that is evolving the Internet’s current host-based packet delivery model.

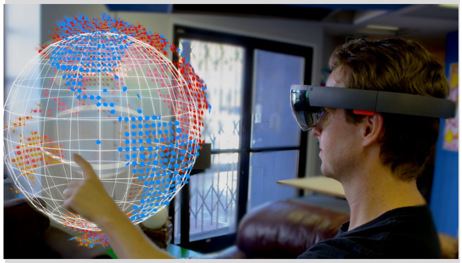
Freeze Attacks in Smart City Surveillance Systems

Freeze attacks, otherwise known as Hollywood attacks, have called attention to the vulnerabilities that exist in various surveillance systems. Smart cities are at high risk because many of these cameras exist in the IoT community, using AWS Deeplens deep learning camera, which provides capabilities for detection functions, testing can be done to identify weaknesses in the developer’s code that make the camera more susceptible to freeze attacks. Also, using the MATLAB image processing toolbox allows for various motion detection programs to be analyzed against movement and stillness. The main drawback of detecting freeze attacks is the inability to recognize one if there are no moving elements within the area of interest. Freeze attacks can be rectified with good programming practice and thorough testing stages.

April 24 Workshop Presentations

Visualization in CPS/IoT with Microsoft Hololens

Today's world has become increasingly connected, digitized, distributed, and diverse, driven by exponential technological growth.



With every "thing" possessing the power to process data, the sheer scale, complexity, and dynamic nature of the day-to-day computer network activities place an unbearable cognitive load on human operators. Visualizing and analyzing threats has profoundly proven to aid in defending computer networks. Hence, based on success in other evolving immersive applications such as the Internet of Things (IoT), Artificial Intelligence (AI) and Machine Learning (ML), Augmented reality holds a promise to improve computer network security operations. We investigate the feasibility of wearable devices' ability to superimpose digital information onto the physical world and provide much needed virtual buttons for accelerated cyber-security synthesis and incidence response, with a focus on the well-established Microsoft Hololens use in a range of visualization applications.

Prediction Based Adaptive RF Spectrum Reservation in Wireless Virtualization

With wireless virtualization, Wireless Infrastructure Providers (WIPs) can sublease out RF spectrum to multiple Wireless Virtual Network Operators (WVNO). The latter can offer services to their customers while sharing the same physical infrastructure. WVNOs are capable of leasing through a reservation process, which may be accompanied by some strict guarantees, usually discouraging overbooking through certain penalties. On a global scale, it is essential for WIPs also to be able to proactively reserve spectrum resources for consumer usage based on informed estimates. As part of the educated estimation, predictions are made from data of previous spectrum allocations and harmonized with an aggregation of crowd-sourced data for events in a bid to reduce the probability of overbooking. The data aggregation effort relies on the reliability of workers to generate accurate results using a community-based aggregation model.

Dependable Adaptive Mobility in Vehicular Networks for Resilient Mobile Cyber-Physical Systems

Transportation systems across the world leverage developments in information and communication technologies and other associated fields to address safety, high mobility, and environmental concerns. This trend, known as intelligent transportation systems (ITS), is characterized by advanced driver-assistance systems like lane departure warning, adaptive cruise control and collision avoidance subsystems. However, in connected and autonomous vehicles, the efficient functioning of these systems depends largely on the ability of a vehicle to predict its operating parameters such as location and speed accurately. The ability to predict the future location (or speed) of a vehicle or its neighbors guarantees integrity, availability, and accountability, consequently boosting security and resiliency of the vehicular cyber-physical system (VCPS). This research proposes algorithms for secure movement-prediction and optimal exchange of information between connected vehicles. The goal is to achieve resilience in the exchange of information between connected vehicles, as they travel adaptively.

A Highly Efficient and Reliable Data Distribution With Tiered Storage Management

PACT
Partnership for Proactive Cybersecurity Research and Training

Derek Major, Kendal Hall, Richelle Javier and Pratik Satam

The research, implementation and development of the project worked on throughout the program deals with OpenVAS technology in relation to computer security. The overall purpose of our research is to see how this open-source tool is used to be able to scan networks and devices for vulnerabilities. Through the use of Virtual machines given to us from EC2 instances on amazon, we've been able to install OpenVAS for scanning machines as well as using another virtual machine to be able to install vulnerabilities for testing. The major findings uncovered throughout this project has been how OpenVAS can be used to generate a report on IP scans of a machine. The report given after successfully configuring a scan is able to give key data points to see how severe vulnerabilities on that IP are. The report can then give information on how to fix these vulnerabilities on a computer and can lessen the risk of one of these vulnerabilities being exploited by a hacker. On a larger scale, this tool can be used to ensure the safety of assets in a network and can ensure that the cyberspace is secure.

Goals

Creating an experiment in a CLasS environment using OpenVAS for experimentation and usage of OpenVAS in the security environment

Configuring vulnerabilities on a separate virtual machine in order to be able to implement IP scans

Need to understand vulnerabilities and how they are detected using OpenVAS technology

Methodologies

Research what OpenVAS is and how it can be used to achieve the project topic goal

Use cloud instances of VMs to get familiar with the Linux environment

Install vulnerabilities onto the virtual machine that will be scanned

Reinstall OpenVAS on a local machine VM because of an Amazon root privilege error

Perform scans on the VMs that has vulnerabilities and see results yield

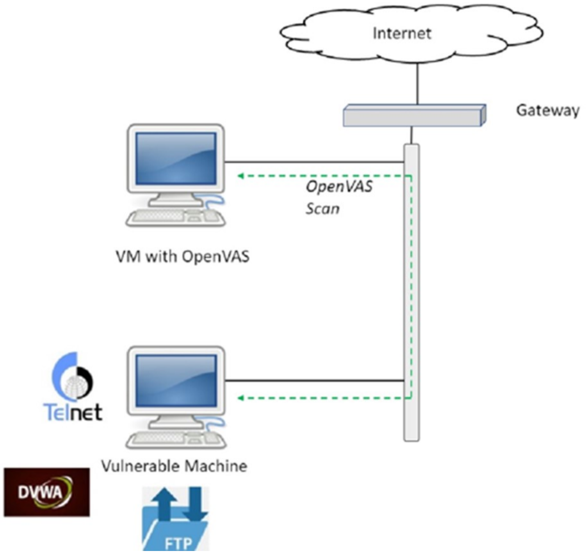
Tools

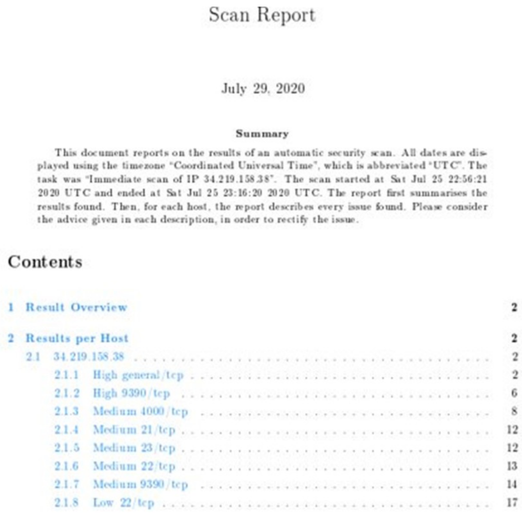
OpenVAS has been utilized as the main tool used to configure IP scans on vulnerable Virtual machines

Telnet is an early network protocol which uses an unencrypted connection over TCP/IP

FTP is a client-server protocol where a client will ask for a file, and a local or remote server will provide it

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that includes a multitude of vulnerabilities





Scan Report

July 29, 2020

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Immediate scan of IP 34.219.158.38". The scan started at Sat Jul 25 22:56:21 2020 UTC and ended at Sat Jul 25 23:16:20 2020 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview 2
2 Results per Host 2
2.1 34.219.158.38 2
2.1.1 High general/tcp 2
2.1.2 High 9390/tcp 6
2.1.3 Medium 4000/tcp 8
2.1.4 Medium 21/tcp 12
2.1.5 Medium 23/tcp 12
2.1.6 Medium 22/tcp 13
2.1.7 Medium 9390/tcp 14
2.1.8 Low 22/tcp 17

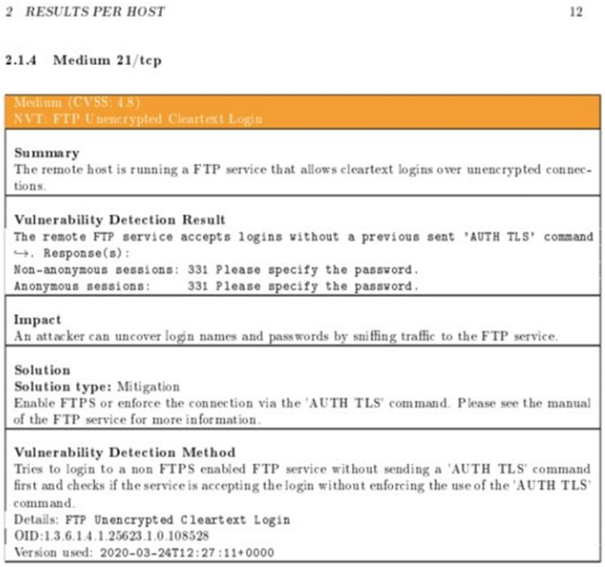
Continue on next page

Results

In this project certain goals and objectives were Telnet Vulnerability: The OpenVAS scan report shows that the Telnet Vulnerability occurs on Port 23/TCP. This will make the computer prone to sniffing attacks and will allow attackers to uncover login names and passwords. The solution is to replace Telnet with a protocol like SSH.

FTP Vulnerability: The OpenVAS scan report shows that the FTP Vulnerability occurs on Port 21/TCP. Similar to Telnet, FTP will also make a computer prone to sniffing attacks. The solution is to enable FTPS.

SSL/TSL Vulnerability: The OpenVAS scan report shows that the SSL/TSL Vulnerability occurs on Port 9390/TCP. This will make the computer prone to man in the middle attacks. The solution is to disable SSLv3.



2 RESULTS PER HOST 12

2.1.4 Medium 21/tcp

Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login

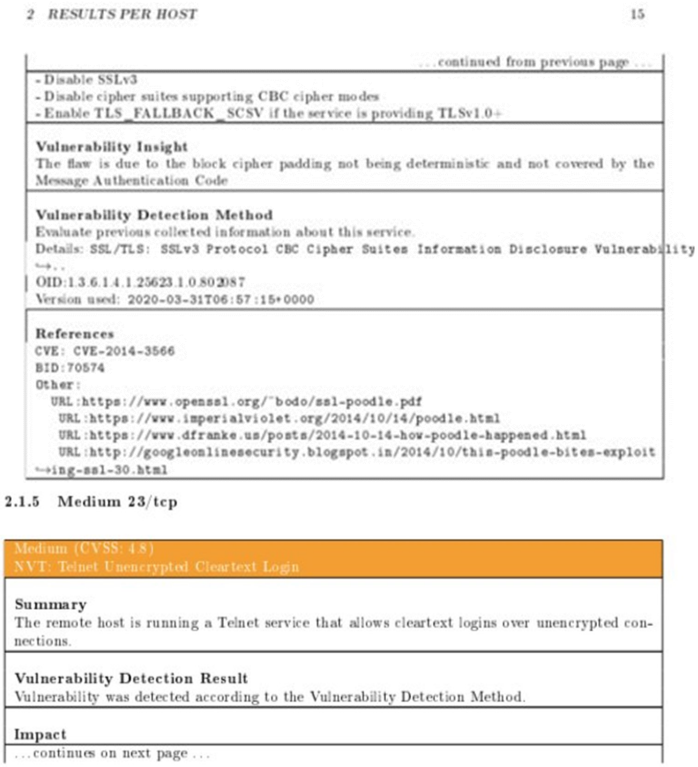
Summary
The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Vulnerability Detection Result
```
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
↪. Response(s):
Non-anonymous sessions: 331 Please specify the password.
Anonymous sessions:     331 Please specify the password.
```

Impact
An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

Solution
Solution type: Mitigation
Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

Vulnerability Detection Method
Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.
Details: FTP Unencrypted Cleartext Login
OID:1.3.6.1.4.1.25623.1.0.108528
Version used: 2020-03-24T12:27:11+0000



2 RESULTS PER HOST 15

. . . continued from previous page . . .

- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes
- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

Vulnerability Insight
The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

Vulnerability Detection Method
Evaluate previous collected information about this service.
Details: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability
↪..
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: 2020-03-31T06:57:15+0000

References
```
CVE: CVE-2014-3566
BID:70574
Other:
  URL:https://www.openssl.org/~bodo/ssl-poodle.pdf
   URL:https://www.imperialviolet.org/2014/10/14/poodle.html
   URL:https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
   URL:http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploit
↪ing-ssl-30.html
```

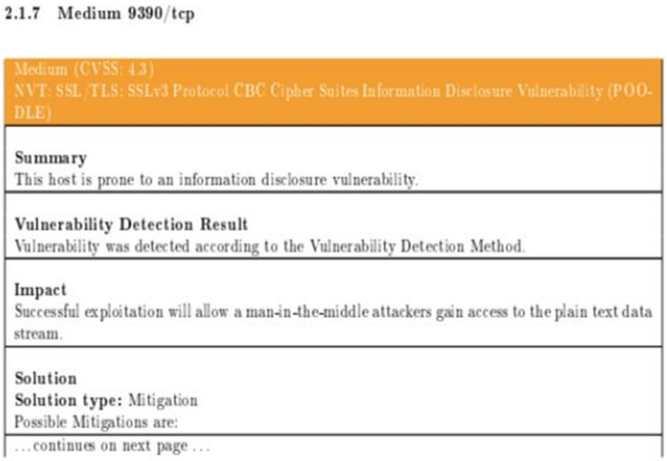
2.1.5 Medium 23/tcp

Medium (CVSS: 4.8)
NVT: Telnet Unencrypted Cleartext Login

Summary
The remote host is running a Telnet service that allows cleartext logins over unencrypted connections.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
. . . continues on next page . . .



2.1.7 Medium 9390/tcp

Medium (CVSS: 4.3)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

Summary
This host is prone to an information disclosure vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.

Solution
Solution type: Mitigation
Possible Mitigations are:
. . . continues on next page . . .

Prediction Based Adaptive RF Spectrum Reservation in Wireless Virtualization

Abdulhamid Adebayo and Danda Rawat, Howard University

Min Song, Stevens Institute of Technology

Summary

With wireless virtualization, Wireless Infrastructure Providers (WIPs) are able to sublease out RF spectrum to multiple Wireless Virtual Network Operators (WVNO) who in turn offer services to their customers while sharing the same physical infrastructure. WVNOs are capable of leasing through a reservation process which may be accompanied by some strict guarantees, usually discouraging overbooking through certain penalties. On a global scale, it is important for WIPs to also be able to proactively reserve spectrum resources for consumer usage based on informed estimates.

In the system model, decisions associated with spectrum reservation are handled by the SDN controller. However, two other components – aggregator and predictor – contribute to the reservation decision making process as shown in Figure 1 below. As part of the educated estimation, predictions are made from data of previous spectrum allocations and harmonized with aggregation of crowd-sourced data for events in a bid to reduce the probability of overbooking. The data aggregation effort relies on the reliability of workers to generate highly accurate results using a community-based aggregation model.

There are three key “reservation” parameters necessary in the spectrum reservation mechanism. The location parameter *l* dictates the location in service footprint/region for which reservation is to be made, the time parameter *t* provides a time duration for the reservation, and the volume parameter *v* provides an estimate for the number of channels to be reserved. These values are obtained as a function of the output from the prediction engine (lp,tp,vp) and an aggregation of the crowd-sourcing effort (lc,tc,vc). The reservation parameters are expressed as:

$$l = \alpha l_p + \beta l_c, \qquad (1a)$$

$$t = \alpha t_p + \beta t_c, \qquad (1b)$$

$$v = \alpha v_p + \beta v_c \qquad (1c)$$

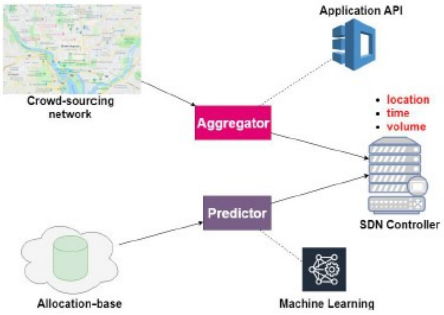


Figure 1: Bi-layer reservation components using machine learning on cloud-based data and secure application API to aggregate crowdsourced data.

obtained as a function of the output from the prediction engine and an aggregation of the crowd-sourcing effort. The reservation parameters are expressed as:

A novel spectrum reservation prediction algorithm – Volume-conditioned Spectrum Selective Moving Average (VSSMA) – is proposed using the trend similarity of spectrum allocation. This approach differs from the Exponential Weighted Moving Average (EWMA) by consolidating allocations in location with high proximity as well as setting a volume threshold to be considered for prediction. The algorithm attempts to achieve more accurate forecasts.

VSSMA uses a couple of strategies to optimize prediction performance. One is the classification of the past alloca-

Continue on page 9

tions based on their satisfaction of the volume threshold. The other is using the Weighted-Average based on similarity. The predicted values are related to the time and location slot in the same day (of prediction) and the selective moving average of the past allocations (same slot in past days).

We validate the desirable properties of the proposed approach through theoretical analysis, as well as simulations.

Figure 2 shows that VSSMA and EWMA both get low error with VSSMA recording lower error due to the similar allocation trends in the allocation data. Also, VSSMA avoids a significant error due to varying allocation volumes by using a selective average.

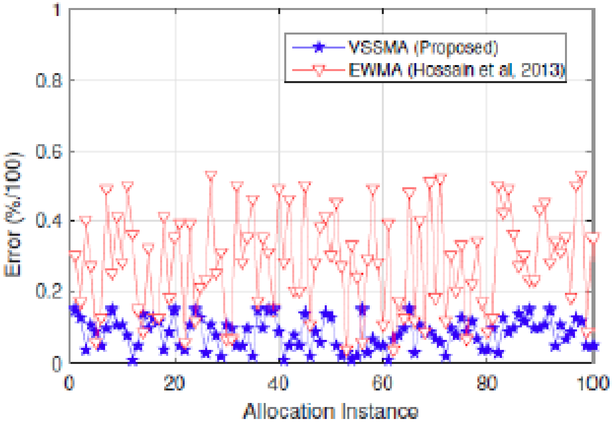


Figure 2: Error in the proposed VSSMA and existing EWMA methods vs allocation instances

Figure 3 shows that the more accurate the prediction is, the closer the predicted volume of resources reserved is to the actual volume needed which overall leads to reduced cost of allocation. When the prediction results in overbooking of resources, it translates to a higher prediction error which has the same effect on the allocation cost due to the increase in the inherent cost of spectrum booking.

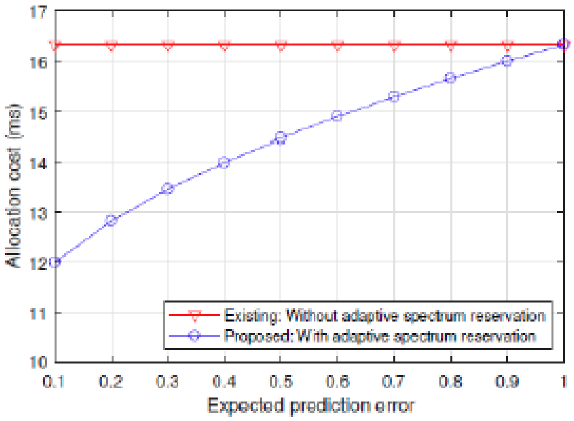
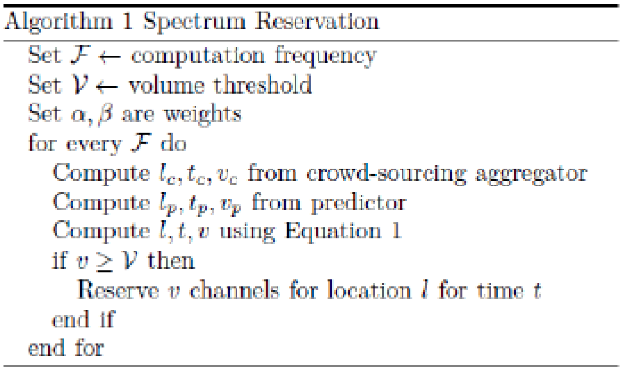


Figure 3: Allocation cost (delay) with proposed approach vs without proposed approach



```
Algorithm 1 Spectrum Reservation
  Set $\mathcal{F} \leftarrow$ computation frequency
  Set $\mathcal{V} \leftarrow$ volume threshold
  Set $\alpha, \beta$ are weights
  for every $\mathcal{F}$ do
    Compute $l_c, t_c, v_c$ from crowd-sourcing aggregator
    Compute $l_p, t_p, v_p$ from predictor
    Compute $l, t, v$ using Equation 1
    if $v \geq \mathcal{V}$ then
      Reserve $v$ channels for location $l$ for time $t$
    end if
  end for
```

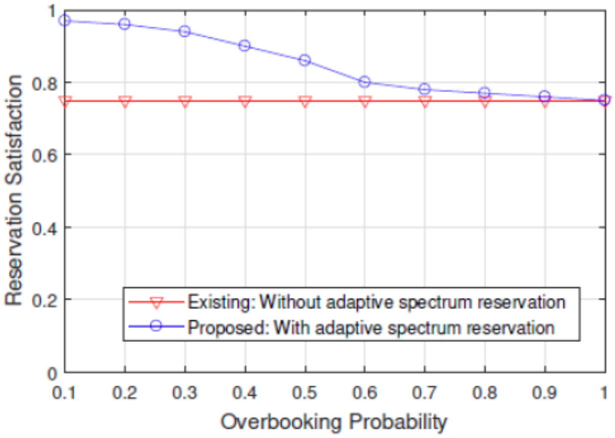


Figure 4: Impact of overbooking on reservation satisfaction

Figure 4 shows the impact of overbooking on reservation satisfaction vs. the overbooking probability. With the adaptive reservation technique proposed in this paper, estimated spectrum volume is closer to the expected value leading to a higher reservation satisfaction compared to when it is not used. The reservation satisfaction value reduces with higher overbooking probability and it is comparable to the satisfaction values when the adaptive reservation is not used as the probability of overbooking increases. This aligns with the goal of this research to reduce the probability of overbooking. satisfaction values when adaptive reservation is not used as the probability of overbooking increases. This aligns with the goal of this research to reduce the probability of overbooking.

Mitigating Data Poisoning Attacks on a Federated Learning-Edge Network

Ronald Doku and Danda Rawat, Howard University

Abstract: Edge Computing (EC) has seen a continuous rise in its popularity as it provides a solution to the latency and communication issues associated with edge devices transferring data to remote servers. EC achieves this by bringing the cloud closer to edge devices. Even though EC does an excellent job of solving the latency and communication issues, it does not solve the privacy issues associated with users transferring personal data to the nearby edge server. Federated Learning (FL) is an approach that was introduced to solve the privacy issues associated with data transfers to distant servers. FL attempts to resolve this issue by bringing the code to the data, which goes against the traditional way of sending the data to remote servers. In FL, the data stays on the source device, and a Machine Learning (ML) model used to train the local data is brought to the end device instead. End devices train the ML model using local data and then send the model updates back to the server for aggregation. However, this process of asking random devices to train a model using its local data has potential risks such as a participant poisoning the model using malicious data for training to produce bogus parameters. In this paper, an approach to mitigate data poisoning attacks in a federated learning setting is investigated. The application of the approach is highlighted, and the practical and secure nature of this approach is illustrated as well using numerical results.

Proposed Approach: In this work, to vet data (determine whether a potential dataset is poisoned or not), an SVM algorithm is employed. We utilize SVM for vetting data because an FL setting provides an advantage over it's centralized counterpart in the sense that, it allows for a proactive approach to data poisoning mitigation. This is because most of the work done in centralized ML systems focus on gathering data from the wild (usually unknown sources). However, the central server would still have access to the dataset. In FL, it is an ML model that has access to the dataset, not the edge server. However, the data sources are known which in turn provides the possibility of vetting the data before it is trained on an ML model. It is imperative to ensure the vetting process does not compromise the client's sensitive data (the foundation on which FL is built on). To this end, a facilitator is employed to serve as the link between the client and the edge server. The facilitator is a lightweight program that possesses an SVM model and other essential features it requires to effectively vet an end-device's dataset in a fair and privacy secure manner. Fig. 1 provides a visual representation of the process.

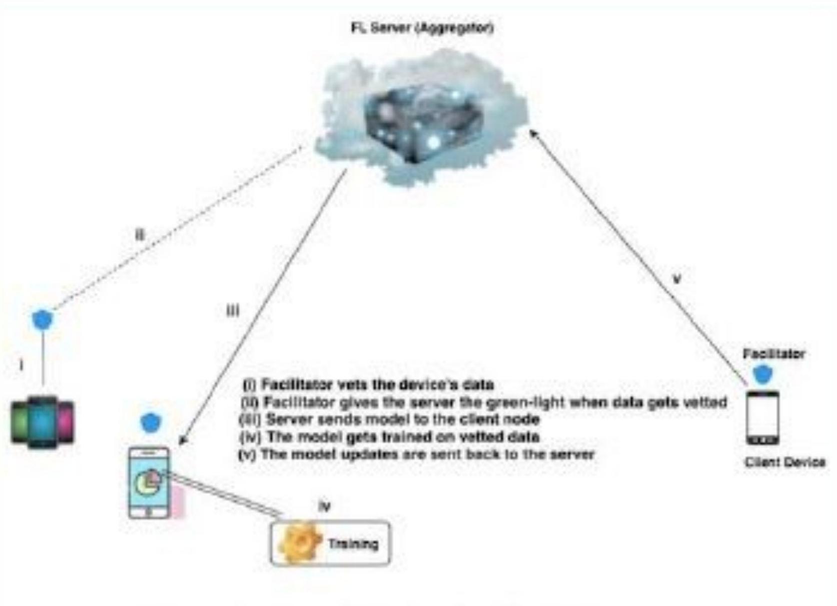

FL Server (Aggregator)
ii
iii
v
i
Facilitator
(i) Facilitator vets the device's data
(ii) Facilitator gives the server the green-light when data gets vetted
(iii) Server sends model to the client node
(iv) The model gets trained on vetted data
(v) The model updates are sent back to the server
Client Device
iv
Training

Figure 1. Data Vetting in the FL Process.

Continue on next page

Mitigating Data Poisoning Attacks on a Federated Learning-Edge Network

Evaluation: Table I shows the precision and recall. We also plot the misdetection rate based on the percentage of falsified data in the dataset (Fig. 2). Our approach performed poorly when the percentage of the flipped label is high, and did reasonably well when the percentage dropped. To test how well our method performed, we generated various data samples each with varying degrees of poisoned data. We had a test group where we train the data on a model after it has passed our vetting process. The control group trained the data without vetting. Fig. 3 is a box and whisker representation of the spread of the accuracy scores across for each model. From these results, it shows the accuracy we get from predicting with the vetted data is better.

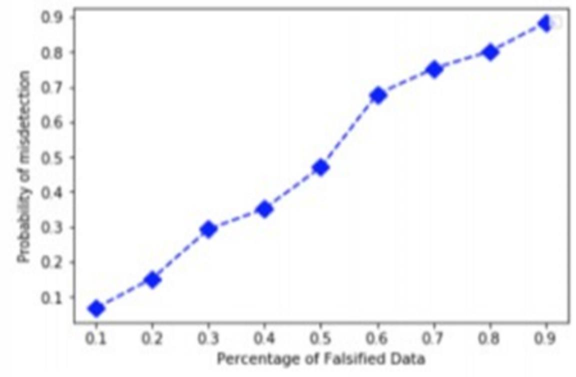


Figure 2. Misdetection

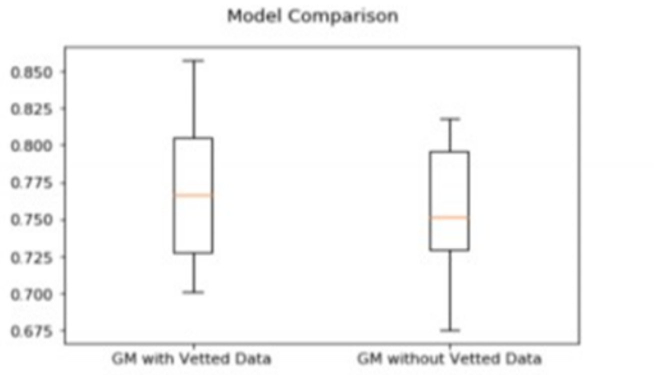
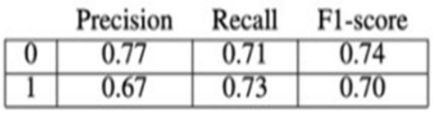


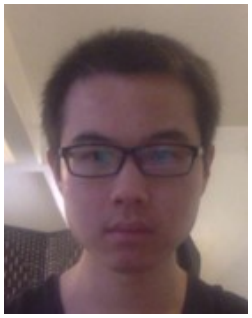
Figure 3. Comparing Model Performance

Table I
PRECISION AND RECALL



	Precision	Recall	F1-score
0	0.77	0.71	0.74
1	0.67	0.73	0.70

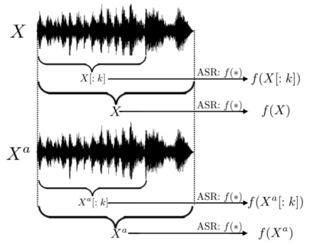
Conclusion: In this paper, we devised an approach that attempts to mitigate the data poisoning issue in a federated learning network. In our approach, we introduce the concept of a facilitator that gets assigned to an end device. The facilitator's job is to ensure the data that an end device owns has not been compromised. It achieves this by employing an SVM model for the data vetting process. We run experiments to determine the effectiveness of our approach. Our experiment showed that a model's accuracy is better when the data it trains on has been positively vetted.



Heng Liu

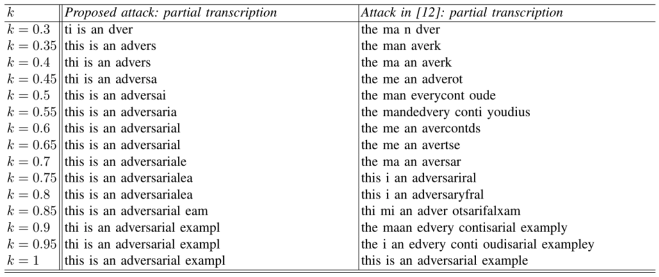
Adversarial Audio Attacks that Evade Temporal Dependency

Heng Liu and Gregory Ditzler, University of Arizona



Example of an audio signal that is designed to fool Mozilla's DeepSpeech translation classifier.

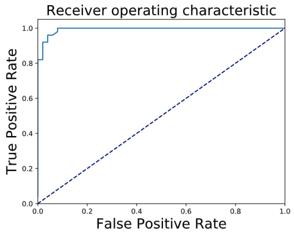
As the real-world applications (image segmentation, speech recognition, machine translation, etc.) are increasingly adopting Deep Neural Networks (DNNs), DNN's vulnerabilities in a malicious environment have become an increasingly important research topic in adversarial machine learning. Adversarial machine learning (AML) focuses on exploring vulnerabilities and defensive techniques for machine learning models. The majority of machine learning (ML) algorithms rely on the assumption that data are sampled from a fixed probability distribution from both the training data. This assumption is often violated in practice, which results in classification and regression strategies that are far from optimal or even reliable, even with neural networks. Furthermore, adversaries have been shown to compromise the machine learning algorithms that go into technologies such as IoT, cybersecurity, etc. As an example, the image on the right shows how a neural network can easily be fooled into making an incorrect translation of an audio signal. In this example, a speech signal is sent to Mozilla's DeepSpeech model for translating the audio signal to text (e.g., technologies that enable Google Home, Amazon's Alexa, etc). The adversary adds a small perturbation to the signal that indistinguishable from the human perception; however, DeepSpeech incorrectly translates the speech. Recent works have developed algorithms to detect such adversarial audio by exploiting temporal dependency in the speech.



k	*Proposed attack: partial transcription*	*Attack in [12]: partial transcription*
$k = 0.3$	ti is an dver	the ma n dver
$k = 0.35$	this is an advers	the man averk
$k = 0.4$	thi is an advers	the ma an averk
$k = 0.45$	thi is an adversa	the me an adverot
$k = 0.5$	this is an adversai	the man everycont oude
$k = 0.55$	this is an adversaria	the mandedvery conti youdius
$k = 0.6$	this is an adversarial	the me an avercontds
$k = 0.65$	this is an adversarial	the me an avertse
$k = 0.7$	this is an adversariale	the ma an aversar
$k = 0.75$	this is an adversarialea	this i an adversariral
$k = 0.8$	this is an adversarialea	this i an adversaryfral
$k = 0.85$	this is an adversarial eam	thi mi an adver otsarifalxam
$k = 0.9$	thi is an adversarial exampl	the maan edvery contisarial examply
$k = 0.95$	thi is an adversarial exampl	the i an edvery conti oudisarial exampley
$k = 1$	this is an adversarial exampl	this is an adversarial example

Example of adversarial signal transcriptions for PI Ditzler's algorithm and an existing adversarial attack that is detectable with temporal dependency.

They focused on generating adversarial audios that are against speech-to-text transcription tasks. We first revisit the LSTM model that is commonly used for performing the transcription then we shed light on the TD's role in generating an adversarial audios' against a speech recognition model. Then we propose a new audio attack algorithm that evades the temporal dependency-based adversarial audio detection and benchmark our algorithm, as well as the state-of-the-art, on the Mozilla dataset. Our results show that our adversarial speech model can evade the temporal dependency detection methods. The table shows example of audio transcriptions for our attack and Carlini's attack. For small values of k, the transcription for Carlini's method is very unreliable, and not even close to the adversarial audio, which is "This is an adversarial sample."



ROC showing the high detection rates of adversarial audio samples

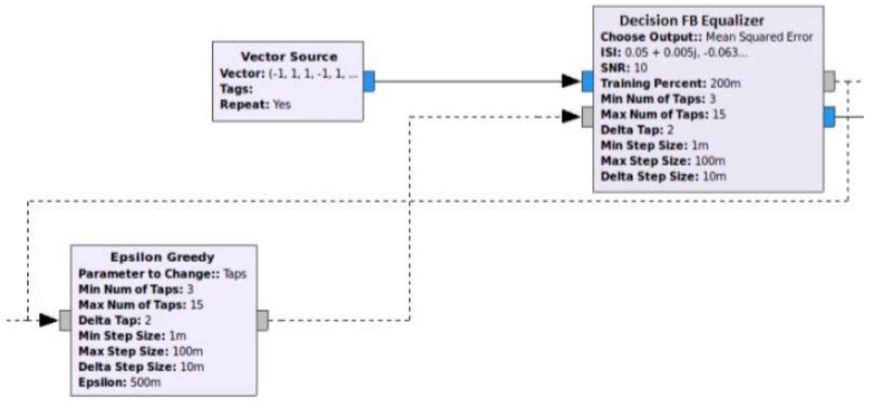
The proposed approach is much closer to the adversarial audio which makes the attack more difficult to detect with temporal dependency. Furthermore, the experiments also show that the adversarial audios remain nearly indistinguishable from benign audios with only negligible perturbation magnitude.

A Suite of Equalizers And Cognitive Engines for Gnu Radio

Melissa Elkadi and Tamal Bose, University of Arizona

Machine learning (ML) has been applied to almost every realm of wireless communications. GNU Radio, an open-source developmental toolkit used to model communication systems has seen few machine learning techniques implemented in its library. This is troubling, as research in communication theory merits the need for such machine learning techniques. One aspect of communication theory that can be improved by machine learning is adaptive equalization. Specifically, machine learning can be used to adjust the structure of an equalizer (i.e. taps, step size, filter type, etc.) to determine optimal equalizer parameters for a specific set of channel conditions. This process is referred to as cognitive equalization. The objective of this work was to demonstrate how cognitive equalization algorithms can be designed and implemented in GNU Radio.

An equalizer is commonly used in wireless systems to reconstruct a signal that may be corrupted due to the nature of the wireless channel. Linear and nonlinear equalizers are used in this work and have their weights updated based on the Least Means Squared (LMS) algorithm. Equalization and machine learning techniques, such as reinforcement learning, can be used with adaptive algorithms to optimize the signal recovery at the receiver. A cognitive engine (CE) is a mechanism that can facilitate the discovery of an optimal structure of a freestanding element in a system. In this work, the cognitive engine will use reinforcement learning techniques to make decisions regarding the structure of an adaptive equalizer.



Vector Source
Vector: (-1, 1, 1, -1, 1, ...
Tags:
Repeat: Yes

Decision FB Equalizer
Choose Output:: Mean Squared Error
ISI: 0.05 + 0.005j, -0.063...
SNR: 10
Training Percent: 200m
Min Num of Taps: 3
Max Num of Taps: 15
Delta Tap: 2
Min Step Size: 1m
Max Step Size: 100m
Delta Step Size: 10m

Epsilon Greedy
Parameter to Change:: Taps
Min Num of Taps: 3
Max Num of Taps: 15
Delta Tap: 2
Min Step Size: 1m
Max Step Size: 100m
Delta Step Size: 10m
Epsilon: 500m

Figure 1: GNU Radio Flowgraph of a Decision Feedback Equalizer and Cognitive Engine

This work began by creating adaptive equalizer blocks, utilizing the LMS algorithm to update the tap coefficient values, in GNU Radio. Once the equalizers' performance was verified, the ε-Greedy cognitive engine block was implemented. The ε-Greedy cognitive engine makes its decisions based on the goal of achieving the highest reward; in this application, the highest reward is obtained by the structure of the equalizer that provides the lowest bit error rate (BER). For example, the structure of the equalizer can be changed to have anywhere from 3 to 15 taps, as shown in Figure 1. The value of ε defines the performance of the CE. ε is a number between [0, 1] that indicates when the CE will randomly explore, and 1- ε indicates when the engine will exploit the various structure options, in search of the highest reward. Figure 1 shows the GNU Radio flow graph and the structure options as a user-provided input range. The Decision Feedback Equalizer and Epsilon Greedy block are custom blocks created in this work; the Vector Source block is a standard GNU Radio block and represents the input data prior to channel effects.

The plot below shows the ε-Greedy cognitive engine block changing the number of taps for a decision feedback equalizer (DFE), based on the BER. The large spikes in BER are indicative of times when the cognitive engine is exploring, or in other words, has selected a random number of taps for the equalizer. When this exploration occurs, the structure of the equalizer is

Continue on next page

Adversarial Filters for Secure Modulation Classification

A. Berian, K. Staab, N. Teku, G. Ditzler, T. Bose, R. Tandon

Modulation Classification (MC) refers to the problem of classifying the modulation class of a wireless signal. In the wireless communications pipeline, MC is the first operation performed on the received signal and is critical for reliable decoding. The paper considers the problem of secure modulation classification, where a transmitter (Alice) wants to maximize MC accuracy at a legitimate receiver (Bob) while minimizing MC accuracy at an eavesdropper (Eve).

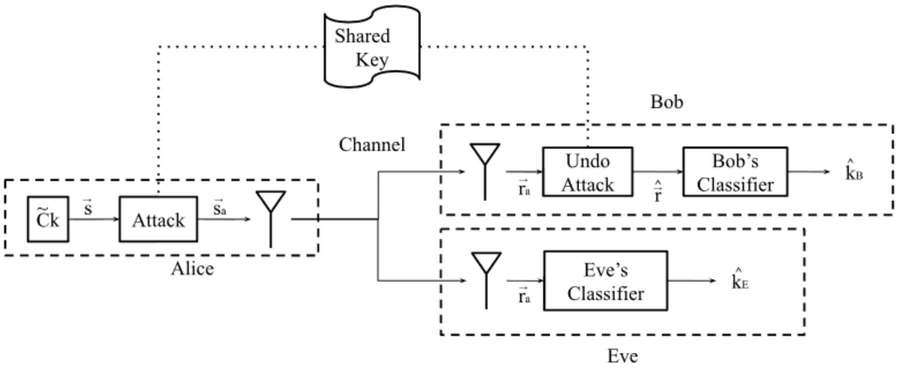


Figure 1: Assumed Communication system model with Transmitter (Alice), receiver (Bob), and eavesdropper (Eve)

The contribution of this work is to design novel adversarial learning techniques for secure MC.

In particular, we present adversarial filtering based algorithms for secure MC, in which Alice uses a carefully designed adversarial filter to mask the transmitted signal, that can maximize MC accuracy at Bob while minimizing MC accuracy at Eve. We present two filtering based algorithms, namely gradient ascent filter (GAF), and a fast gradient filter method (FGFM), with varying levels of complexity. Our proposed adversarial filtering based approaches significantly outperform additive adversarial perturbations (used in the traditional ML community and other prior works on secure MC) and also have several other desirable properties. In particular, GAF and FGFM algorithms are a) computational efficient (allow fast decoding at Bob), b) power-efficient (do not require excessive transmit power at Alice); and c) SNR efficient (i.e., perform well even at low SNR values at Bob).

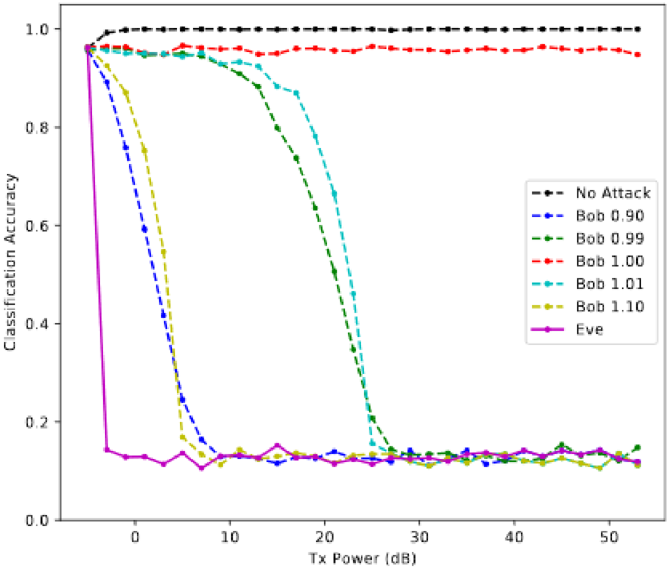


Figure 2: The relationship between Alice's transmit power and Eve/Bob's classification accuracy when noise power is5dB and the minimum SNR requirement at Bob is 0dB.

This paper concludes that additive adversarial attacks fall short in this application, because they require sacrificing transmit power, and can be difficult to undo for Bob. To undo an additive perturbation, Bob must synchronize the subtraction of the perturbation with Alice's repeated addition of the perturbation .

This paper proposes three methods of creating a GAF, two of which have a stable inverse which is necessary for Bob to decode information. The second presented AL filtering algorithm is similar to the fast gradient method (FGM), called the fast gradient filter method (FGFM). In simulations with a convolutional neural network, the root training GAF was the most effective AL algorithm in this system model where transmit power is limited.

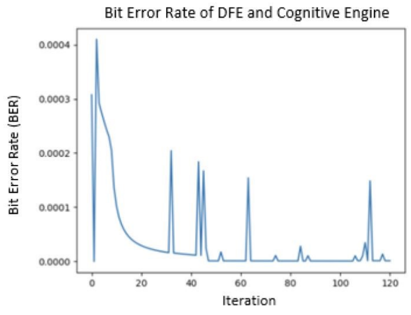


Figure 2: BER of the Decision Feedback Adaptive Equalizer with the Cognitive Engine Changing the number of Taps (Epsilon = 0.2)

not guaranteed to be optimal but exploration is critical in the decision making process of the CE, as it ensures that the optimal structure is not overlooked. Overall, the cognitive engine maintains a BER close to the known optimal structure, in this case it is 11 taps, resulting in a BER near 1x10-5. Cognitive equalization is valuable for the performance of an equalizer because it can update the filter's structure and parameters based on various channel effects impacting the signal.

(continue from the previous article)

Cihan Tunc

The Use of Federated Cybersecurity Testbed as a Service (FCTaaS)

Cihan Tunc, University of Arizona

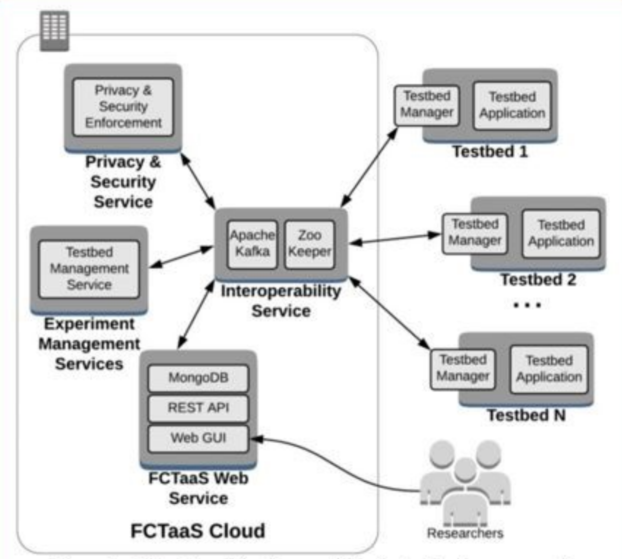


Figure 1. FCTaaS architecture and the individual components

The use of smart infrastructures, with the integration of digital devices and controls, provides better use of the resources. However, this integration also brings multiple vulnerabilities compared to the traditional isolated environments. Hence, there is an urgent need to study these environments in terms of their management and cybersecurity. Studying cybersecurity of the smart infrastructures requires multiple complex testbeds that can show how an attack can propagate, which is extremely difficult to own for an organization alone. Therefore, in this project, we introduce Federated Cybersecurity Testbed as a Service (FCTaaS) for facilitating integration of isolated, geographically dispersed cybersecurity testbeds whether it is physical or virtual, under single federation for researchers and educators to create, perform, reproduce cybersecurity experiments within policies set by the cybersecurity testbeds operators. Therefore, FCTaaS will significantly reduce the experimenters' efforts to discover individual testbeds, create a federated cybersecurity testbed, and then perform the desired cybersecurity experiments as the integrated cybersecurity testbeds can be easily browsed and the experiments can be performed through FCTaaS web interface. Our FCTaaS architecture is shown in Fig. 1 to provide the following services: 1) Interoperability Service – to allow different testbeds to interoperate correctly even if each testbed might use different semantics and terminology through Testbed Manager as it provides a standardized way for exchanging events within FCTaaS environment; 2) Privacy and Security Service – to ensure that the testbeds within federation maintain the required privacy and security policies associated with each testbed that might be governed by different organizations. This service can play an important role within FCTaaS as organizations may want to maintain control of their testbeds to a certain degree which can be done through access policies within FCTaaS environment; 3) Experiment Management Service – to allow users to create and manage their cybersecurity experiments through the connected cybersecurity testbeds under FCTaaS; and 4) FCTaaS Web Service – to provide a ubiquitous user interface to FCTaaS so that the users can have access from anywhere, any time, and using any device (mobile or stationary) with the Internet connectivity.

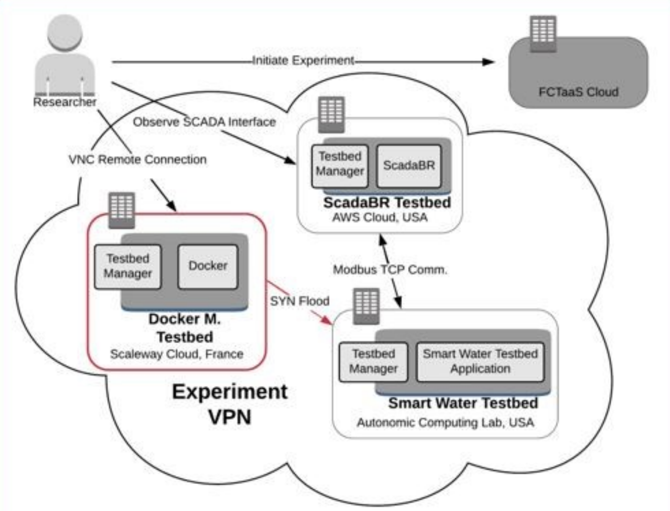


Figure 2. FCTaaS experiment scenario example

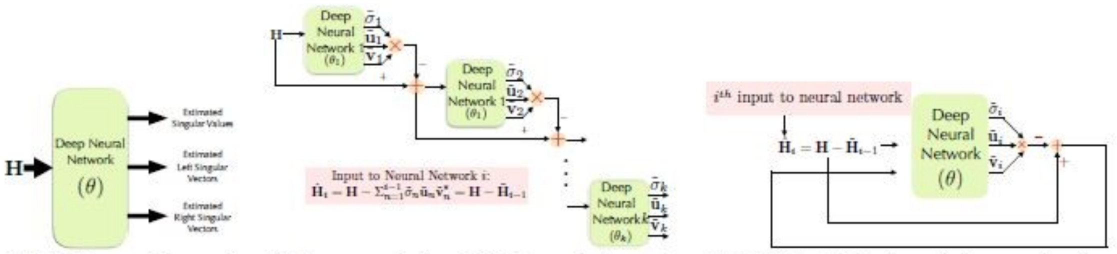
Fig. 2 depicts a scenario where *Smart Water Testbed* represents the critical infrastructure component, the *ScadaBR Testbed* represents the control and management system used by critical infrastructure operators, and the *Docker Management Testbed* represents that attacker who launches SYN flood attack on Smart Water System. This allows the users to create a federated testbed setup to explore different experiments such as answering "What is the necessary DoS bandwidth for an intruder to take down critical infrastructure services?"

Deep Learning for SVD and Hybrid Beamforming

Ture Peken, Sudarshan Adiga, Ravi Tandon, and Tamal Bose
University of Arizona

The underutilized millimeter-wave (mmW) spectrum, along with the massive MIMO, will play a critical role in the next-generation wireless systems to achieve high data rates on the order of 100 Gigabits per second (Gbps) [1]. Large-scale antenna systems (massive MIMO) can focus the radiated energy toward the specific directions by using directional beamforming (BF), which traditionally has been performed either in RF or BB domain. Among the two, digital BF provides higher data rates; however, it requires a large number of RF chains, leading to increased power consumption and cost. On the other hand, analog BF requires fewer RF chains while it compromises on the achievable data rate. The key idea behind hybrid BF is to use a combination of analog and digital BF, with the ultimate goal of keeping the power consumption low, and data rates high [2]. Optimal unconstrained beamformers (which maximize channel capacity) can be found through the singular-value decomposition (SVD) of the channel, i.e., k singular vectors corresponding to the largest singular values of the channel matrix can be used to determine k optimum beam directions. Since SVD-based unconstrained BF provides an upper bound on the maximum achievable rate, finding the optimal hybrid BF solution can be formulated as a constrained SVD problem. Motivated by the recent success of ML/AI in various areas such as image/speech recognition, computer vision, we devise a novel deep neural network (DNN) based framework for singular value decomposition (SVD) and hybrid BF. We first propose three novel DNN architectures with different levels of complexity to learn the unconstrained SVD in supervised manner. Consider a transceiver with a channel denoted by an NR x NT matrix H. Our first proposed approach is to design a DNN architecture seen in Figure 1-a for the rank-k approximation of H. This DNN architecture is trained in a supervised manner by using channel matrices as inputs, and the output data being singular values and vectors. A second DNN architecture given in Figure 1-b has been proposed to reduce the complexity of the supervised DNN for rank-k matrix approximation by concatenating k DNNs. The second architecture consists of k low-complexity DNNs; each DNN is trained to estimate the largest singular value and corresponding right and left singular vectors of the given matrix. We further reduce the complexity by proposing the DNN for rank-1 approximation given in Figure 1-c, which estimates k singular values and singular vectors using a single DNN recursively.

We then consider a hybrid BF system depicted in Figure 2. We consider the case where finite-precision phase shifters are used in the RF domain, which restricts the analog beamformers to have constant modulus and quantized phase values. We propose a novel DNN architecture for hybrid BF as shown in Figure 3 by incorporating these constraints.


H
Deep Neural Network
(θ)
Estimated Singular Value
Estimated Left Singular Vectors
Estimated Right Singular Vectors
H
Deep Neural Network 1 (θ_1)
$\bar{\sigma}_1$
$\bar{\mathbf{u}}_1$
$\bar{\mathbf{v}}_1$
Deep Neural Network 1 (θ_1)
$\bar{\sigma}_2$
$\bar{\mathbf{u}}_2$
$\bar{\mathbf{v}}_2$
Input to Neural Network i:
$\hat{\mathbf{H}}_i = \mathbf{H} - \Sigma_{n=1}^{i-1}\bar{\sigma}_n\bar{\mathbf{u}}_n\bar{\mathbf{v}}_n^* = \mathbf{H} - \bar{\mathbf{H}}_{i-1}$
Deep Neural Networkk (θ_k)
$\bar{\sigma}_k$
$\bar{\mathbf{u}}_k$
$\bar{\mathbf{v}}_k$
i^{th} input to neural network
$\hat{\mathbf{H}}_i = \mathbf{H} - \bar{\mathbf{H}}_{i-1}$
Deep Neural Network
(θ)
$\bar{\sigma}_i$
$\bar{\mathbf{u}}_i$
$\bar{\mathbf{v}}_i$

(a) DNN for rank-k matrix approximation.

(b) Low-complexity DNN for rank-k matrix approximation.

(c) DNN for SVD via rank-1 approximation.

Figure 1: DNN architectures for SVD.

Continue on page 15

Quantization layers are included in the proposed DNN for hybrid BF. However, incorporating quantization brings additional challenges due to the non-differentiability of the discretization operation. In particular, when we use gradient-based optimization methods for training, the quantization layers in DNNs produce zero gradients. To circumvent this issue, we propose four quantization approaches. Finally, we satisfy the power constraint through normalization layers in the proposed DNN architecture.

We then have compared our DNN based approach for hybrid BF with conventional hybrid BF algorithms given in [3{5], and a DL based hybrid BF algorithm in [6]. We see in Figure 4 that the proposed DNN based approach achieves 31:04%, 39:9%, and 24:22% gain in achievable rates compared to state-of-the-art techniques for 4 X 4, 8 X 8, 16 X 16 MIMO, respectively.

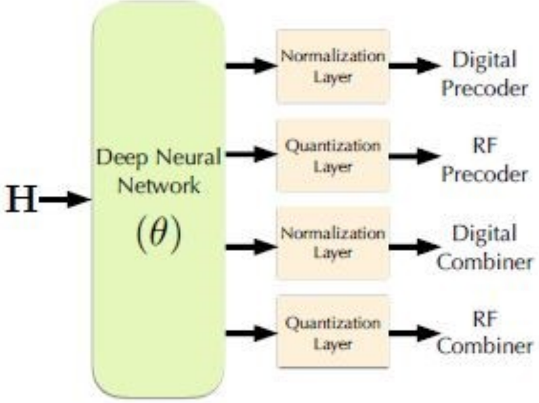


Figure 3: DNN architecture for hybrid BF.

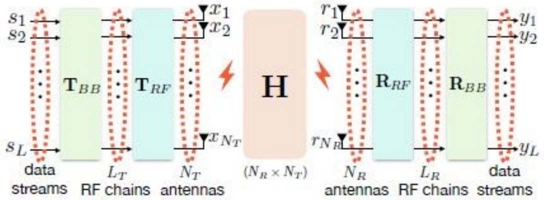


Figure 2: Hybrid BF architecture with RF and baseband blocks at the transmitter and receiver.

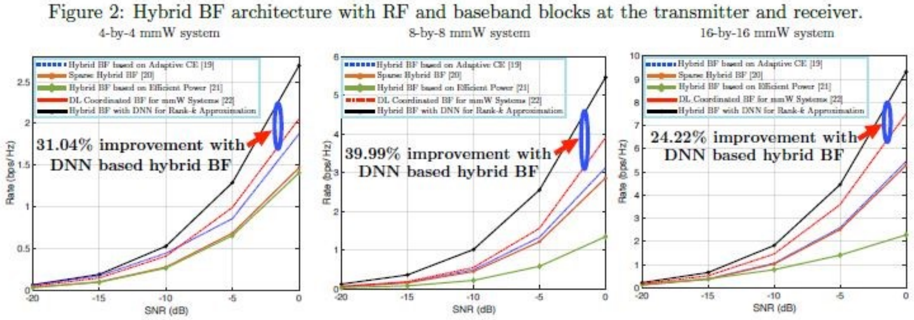


Figure 4: Achieved rates of DNN based hybrid BF, conventional hybrid BF algorithms given in [3–5], and the DL based hybrid BF algorithm given in [6].

In the future, we aim to explore the unsupervised techniques such as generative adversarial networks (GANs) for the SVD and hybrid BF to eliminate the need for supplying valid singular values and singular vectors, which leads to reduced overhead.

References:

[1] T. S. Rappaport, Y. Xing, O. Kanhere, S. Ju, A. Madanayake, S. Mandal, A. Alkhateeb, and G. C. Trichopoulos, \Wireless communications and applications above 100 ghz: Opportunities and challenges for 6g and beyond," IEEE Access, vol. 7, pp. 78 729{78 757, 2019.

[2] A. F. Molisch, V. V. Ratnam, S. Han, Z. Li, S. L. H. Nguyen, L. Li, and K. Haneda, \Hybrid Beamforming for Massive MIMO: A Survey," IEEE Communications Magazine, vol. 55, no. 9, pp. 134{141, Sep. 2017.

[3] A. Alkhateeb, O. E. Ayach, G. Leus, and R. W. H. Jr., \Channel Estimation and Hybrid Precoding for Millimeter Wave Cellular Systems," CoRR, vol. abs/1401.7426, 2014.

[4] O. E. Ayach, S. Rajagopal, S. Abu-Surra, Z. Pi, and R. W. Heath, \Spatially Sparse Precoding in Millimeter Wave MIMO Systems," IEEE Transactions on Wireless Communications, vol. 13, no. 3, pp. 1499{1513, March 2014.

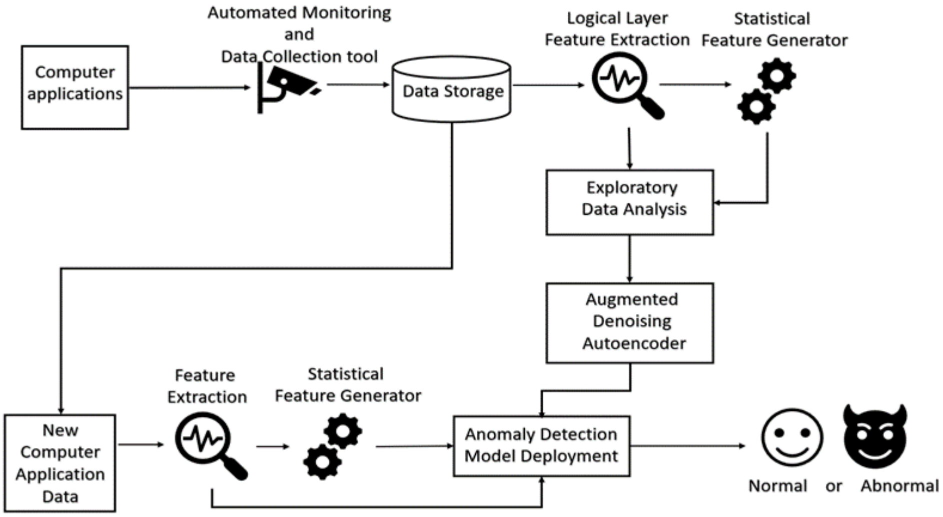
[5] J. Singh and S. Ramakrishna, \On the Feasibility of Codebook-Based Beamforming in Millimeter Wave Systems With Multiple Antenna Arrays." IEEE Trans. Wireless Communications, vol. 14, no. 5, pp. 2670{2683, 2015.

[6] A. Alkhateeb, S. Alex, P. Varkey, Y. Li, Q. Qu, and D. Tujkovic, \Deep Learning Coordinated Beamforming for Highly-Mobile Millimeter Wave Systems," CoRR, vol. abs/1804.10334, 2018.

Machine Learning for Application and Host Security

Sicong Shao, University of Arizona

Cyberspace includes a wide range of physical networks, storage and computing devices, applications, and users with different roles and requirements. Securing and protecting such complex and dynamic cyberspace resources and services are grand challenges. It is well-known that it is very difficult to create security solutions that can protect all the cyberspace layers; i.e., physical, application, and user. Therefore, in this project, we are taking the first steps to create a multi-layer anomaly behavior analysis of components associated with different cyberspace layers and how they interact with each other in order to achieve superior capabilities in characterizing their normal operations and proactively detect any anomalous behavior that might be triggered by malicious attacks. Therefore, in this research, we present an augmented denoising autoencoder anomaly (ADAE) detection technique to intrusion detection system (IDS) for application and host. The architecture of our anomaly detection technique for intrusion detection is shown in Figure 1.


Computer applications
Automated Monitoring and Data Collection tool
Data Storage
Logical Layer Feature Extraction
Statistical Feature Generator
Exploratory Data Analysis
Augmented Denoising Autoencoder
New Computer Application Data
Feature Extraction
Statistical Feature Generator
Anomaly Detection Model Deployment
Normal
or
Abnormal

For the continuous monitoring for application and host, we created a monitoring tool that collects system resource utilization, active software and their resource usage, and user activities. In our approach, we also leverage existing network monitoring tools as well as system monitoring tools to collect information about software systems and their usage patterns. We also use exploratory data analysis (EDA) to explore data to attain a better understanding of normal and abnormal behaviors. Our EDA builds upon principal component analysis (PCA) that is a dimensionality reduction technique used for data visualization. Then, we propose ADAE detection technique (see Figure 2) by learning the features through autoencoder-based anomaly detection techniques. We improved autoencoder-based anomaly detection model by adding different l2 regularization methods to a denoising autoencoder. Further, inspired by the highly successful for applying ReLU with the dropout technique in computer vision and acoustic modeling domain, we applied ReLU with dropout to our anomaly detection model to further improve the detection performance.

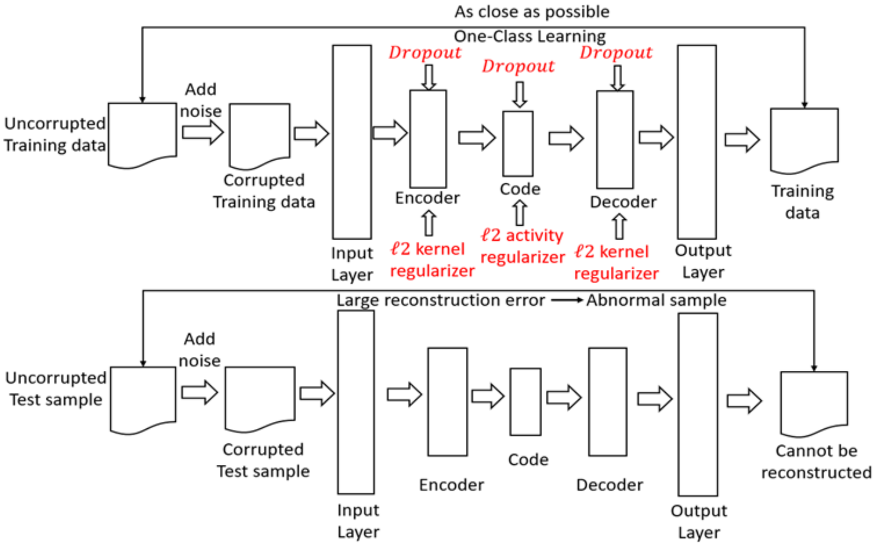


Fig. 2. The architecture of augmented denoising autoencoder

SeVA:
Age-friendly care platform connecting seniors, caregivers, healthcare and community via AI

Chongke Wu, University of Arizona

As a dangerous syndrome, delirium affects more than 50% hospitalized patient and cause 164 billion US dollars lost per year. It is crucial to keep the monitoring system working in a timely way so that the medical staff can give the patient early treatment. The advancement of the Internet of Things in the medical area brings more information to the physician to monitor the patient's status and decision-making; however, it also causes the information-overloaded and alerts overloaded. The renaissance of Artificial Intelligence brings the chance to analyze a large amount of monitoring data. The deep neural network like Convolutional Neural Network and Recurrent Neural Network revolutionizes the field like Computer Vision and Natural Language Processing. Deep learning tasks like action recognition, language understanding can be part of the routine of regular hospital check. With the assistance of deep learning technologies, we propose a chatbot based monitoring system to relieve the medical staff workload by using the Artificial Emotional Intelligence platform. The system includes two mobile applications that provide timely patient monitoring, regular checking, and health status recording features. Compared to the conventional monitoring system, we demonstrate the system superiority in the hospital environment.

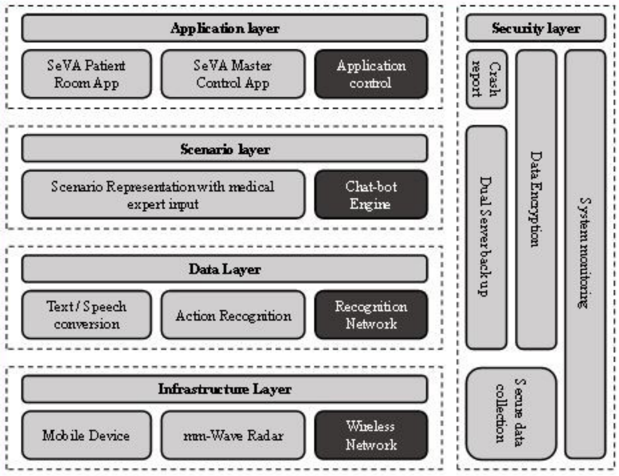


Fig. 1. System Framework of SeVA. The dark background block represents the foundation or necessary utility of our technologies.

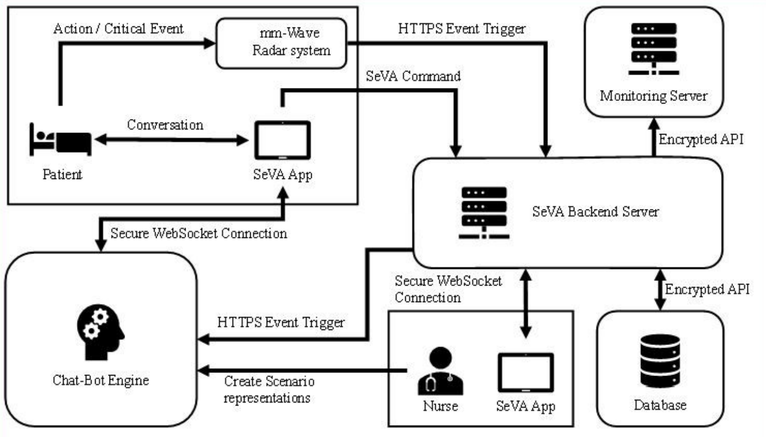


Fig. 2. System Architecture of SeVA. The arrow direction represnts the information flow direction

There has been a mobile version of the SeVA AI Agent which has been developed. In this app is an age-friendly virtual assistant with emotional intelligence. SeVA considering the medical background of the rehabilitation practice, including dementia prevention and fall prevention. We have introduced SeVA architecture and current progress and deliverable. Also, we will how the mobile app is deployed in the related functionality. With the demonstration of SeVA, you will learn how mobile development being helpful for the research project.

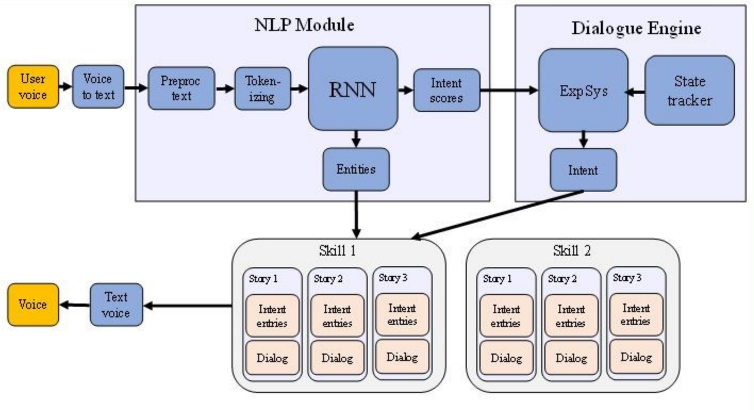


Fig. 3. AEI Chatbot engine architecture.

Multilevel Bluetooth Intrusion Detection System

Shalaka Satam, University of Arizona

Problem:

The rapid deployment of IoT devices has made Bluetooth (IEEE 802.15.1) the wireless network of choice for close-range/ indoor communications. Bluetooth network finds its primary use in the delivery of audio streams to speakers, connecting peripheral devices like keyboards, and in connecting wearables like smartwatches, heart monitors to their controllers. Bluetooth devices use FHSS over 79 frequencies and operate in a Master/Slave configuration. A master can connect up to 7 slave devices to form a Piconet. A slave device can be part of multiple Piconets to form scatter-nets, as shown in figure 1. In hospitals and offices, devices communicate with one another, sharing sensitive and critical information over Bluetooth scatter-nets, making it necessary to secure these Bluetooth networks against attacks like Man in the Middle attack (MITM), eavesdropping attack, and Denial of Service (DoS) attacks. As a part of this research, we are developing a Multi-Level Bluetooth Intrusion Detection System (IDS) to secure the Bluetooth protocol. This IDS is not only able to detect attacks on Bluetooth protocols with precision up to 99.6% and recall up to 99.6% but is also able to perform whitelisting to prevent unauthorized devices from connecting to the network.

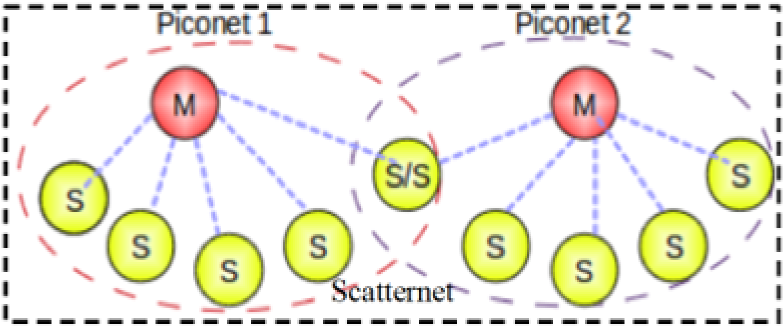


Figure 1. Bluetooth Scattternet

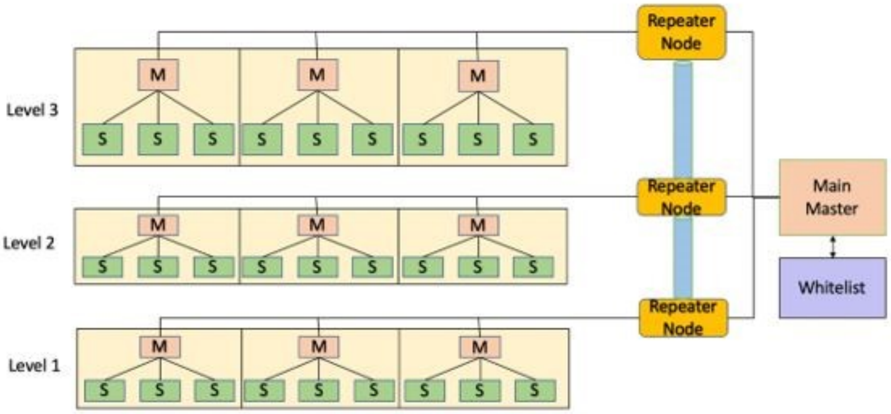


Figure 2: Architecture of Multilevel Bluetooth Network

Approach:

Figure 2 shows the architecture of the Multi-Level Bluetooth Intrusion Detection System (MLBIDS). In the figure, multiple Bluetooth piconets connected to one another over wired networks form a large Bluetooth network used to share information. The networks are split into different levels based on the criticality of the connected devices and the importance of the data shared. The Bluetooth Behavior Analysis Unit (Figure 3) is deployed on the master of each Blue-

Continue on page 19

tooth piconet to secure the piconet against attacks like Man in the Middle and Denial of Service attacks. When a new device tries to connect to the Bluetooth network, the MLIDS performs device authentication and whitelisting by all piconet masters forwarding all the connection requests to a Master Whitelisting Server (MWS), which authenticates each connecting device with into the piconets based on device identity and piconet level.

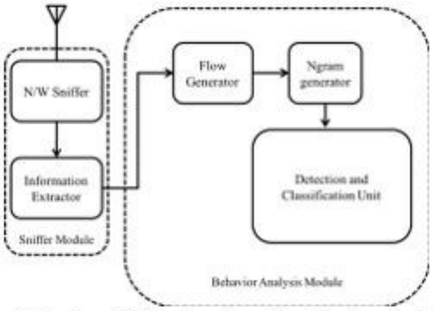


Figure 3. Bluetooth Behavior Analysis Architecture

The Bluetooth Behavior Analysis Unit (BBAU) consists of a sniffer module and behavior analysis module. The Sniffer module collects the Bluetooth frames from the wireless medium, processes the collected frames and passes the processed frames to the Behavior Analysis Module. The Behavior Analysis Module analyses the behavior of the received Bluetooth frames. The data received is split into Observation-flows of size t seconds. The observation-flow is then converted to n-grams. The probability of that observed n-gram being either normal or abnormal is calculated using predetermined heuristics methodologies.

Results:

The presented Bluetooth Behavior Analysis Unit was deployed on a Bluetooth network to detect attacks. The Bluetooth Behavior Analysis architecture was testing with eavesdropping and Denial of Service (DoS) attacks like BlueSnarfing and Power Draining attacks. Figure 4a, 4b, and 4c show the performance of the IDS. From the results presented in Figure 4a-c, conclude that the presented architecture is able to detect attacks with very high accuracy and low false positives and negatives.

The performance of the whitelisting approach was measured similarly to detect and prevent unauthorized devices from connecting to the network. The whitelisting approach was successfully able to detect and prevent unauthorized devices from connecting to the network.

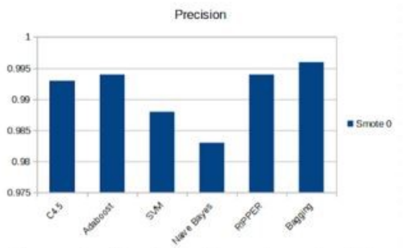


Figure 4.a: Precision for various classifiers

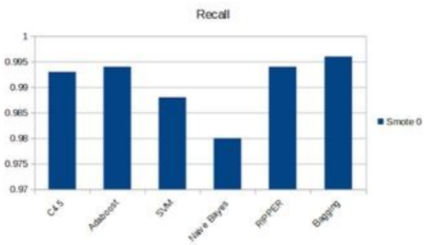


Figure 4.b: Recall for various classifiers

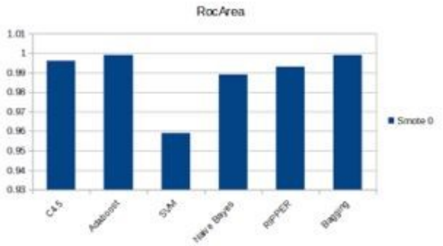


Figure 4.c: RoC area for various classifiers

Publications and Presentations

Accepted

1) T. Peken, S. Adiga, R. Tandon, and T. Bose, (2020) “Deep Learning for SVD and Hybrid Beamforming,” IEEE Transactions on Wireless Communications, accepted for publication in June 2020.
2) K. Jung, S. Spillane, K. Bowers, T. Peken, M. Marefat, T. Bose, (2020) "Machine Learning-Based MIMO Equalizer for High Frequency (HF) Communications", International Joint Conference on Neural Networks.
3) Shao, Sicong, Cihan Tunc, Amany Al-Shawi, and Salim Hariri, (2020) "Ensemble of Ensemble Learning-based Author Attribution for Internet Relay Chat Forensics," ACM Transactions on Management Information Systems (TMIS)

Submitted

1) Shao, Sicong, Cihan Tunc, Amany Al-Shawi, and Salim Hariri, (2020) "Ensemble of Ensemble Learning-based Author Attribution for Internet Relay Chat Forensics," ACM Transactions on Management Information Systems (TMIS).
2) Z. Sadeq, T. Peken, T. Bose, (2020) “A Survey on Wireless Security of 6G: On the Path to AI-Enabled Wireless Networks,” submitted to the International Telemetering Conference.
3) A. Berian, K. Staab, N. Teku, R. Tandon, T. Bose, G. Ditzler (2020) “Adversarial Filtering for Secure Modulation Classification,” submitted to the ArXiv
4) A. Berian, K. Staab, T. Bose, G. Ditzler (2020) “Polynomial Filtering for Secure Modulation Classification” submitted to the International Telemetry Conference
5) Q. Nguyen, M. Elkadi, A. Berian, T. Bose, (2020) “Multichannel neural network equalizers,” submitted to the International Telemetering Conference.

Published

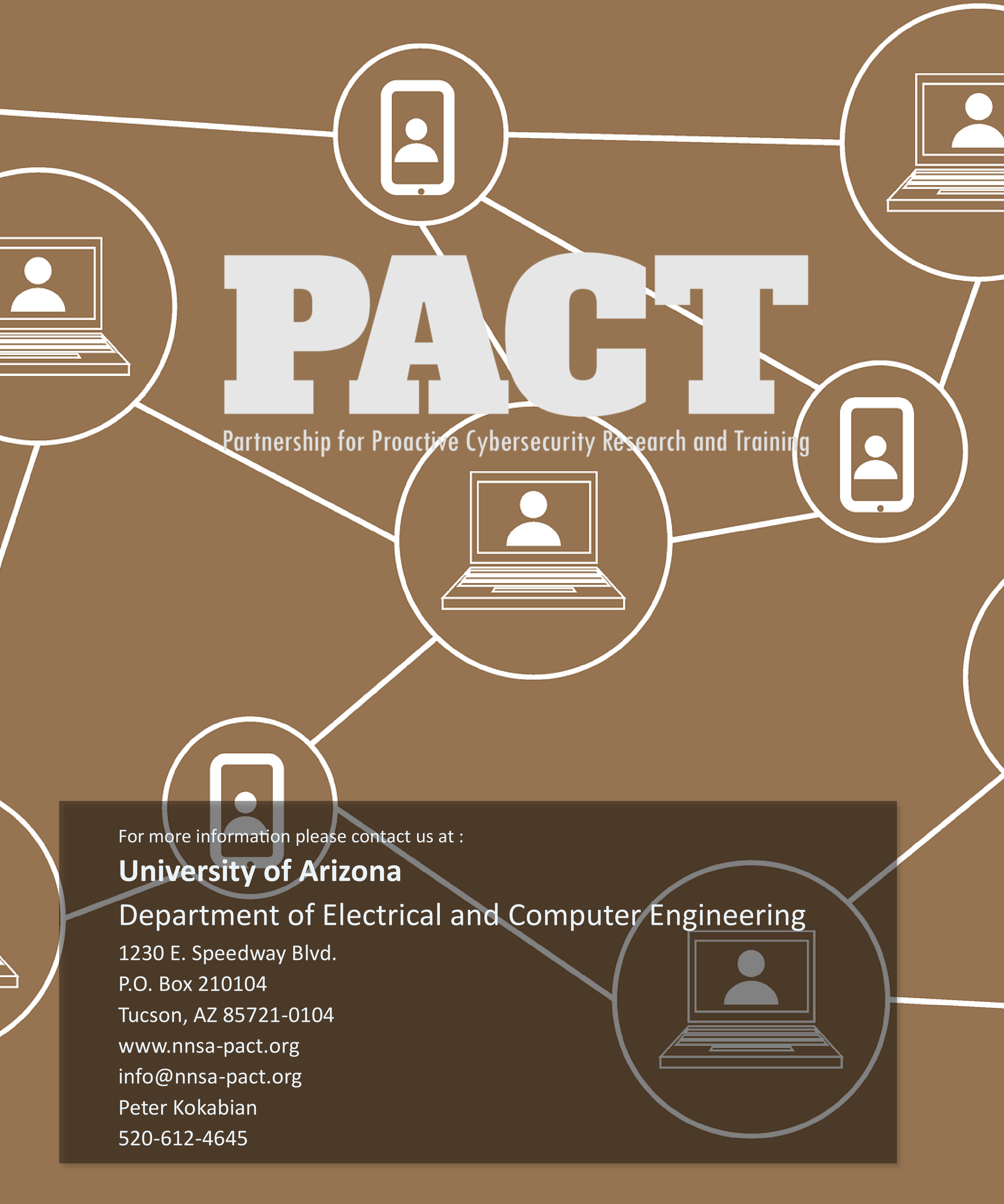
1) T. Peken, R. Tandon, and T. Bose, (2020) “Unsupervised mmWave Beamforming via Autoencoders,” in the Proceedings of the IEEE International Conference on Communications (ICC), June 2020.
2) T. Peken, R. Tandon, and T. Bose, (2019) "Reinforcement Learning for Hybrid Beamforming in Millimeter Wave Systems," in the Proceedings of the International Telemetering Conference, October 2019.
3) Ronald Doku and Danda B. Rawat, "iFLBC: On the Edge Intelligence Using Federated Learning Blockchain Network," Proc. of the 5th IEEE International Conference on Intelligent Data and Security (IEEE IDS 2020), May 25-27, 2020, Baltimore, USA

Publications and Presentations

4) F. O. Olowononi, D. B. Rawat and C. Liu, "Dependable Adaptive Mobility in Vehicular Networks for Resilient Mobile Cyber Physical Systems," Proc. of the IEEE ICC 2020 Workshop on Secure and Dependable Software Defined Networking for Sustainable Smart Communities, 7-11 June 2020, Dublin, Ireland.
5) Ronald Doku, Danda B. Rawat and Chunmei Liu, "On the Blockchain-Based Decentralized Data Sharing for Event-Based Encryption to Combat Adversarial Attacks,"
6) IEEE Transactions on Network Science and Engineering, Vol. x, No. x, pp. xxx-xxx, 2020.
7) K.S. Peng, G. Ditzler and J. Rozenblit, (2019) "Self-Supervised Correlational Monocular Depth Estimation using ResVGG Network," International Conference on Intelligent Systems and Image Processing
8) G. Ditzler, S. Miller, and J. Rozenblit, (2019) "Learning What We Don't Care About: Regularization with Sacrificial Functions," Information Sciences, vol. 496, pp. 198-211.
9) H. Liu and G. Ditzler, (2019) "A Semi-Parallel Framework for Greedy Information-Theoretic Feature Selection," Information Sciences, vol. 492, pp. 13-28.
10) Shao, Sicong, Cihan Tunc, Amany Al-Shawi, and Salim Hariri, (2019) "One-Class Classification with Deep Autoencoder Neural Networks for Author Verification in Internet Relay Chat." In 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), pp. 1-8. IEEE.
11) Shao, Sicong, Cihan Tunc, Amany Al-Shawi, and Salim Hariri, (2019) "Automated Twitter Author Clustering with Unsupervised Learning for Social Media Forensics." In 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), pp. 1-8. IEEE.

Presented

1) A. Berian, I. Aykin, M. Krunz and T. Bose, "Deep Learning-Based Identification of Wireless Protocols in the PHY layer," 2020 International Conference on Computing, Networking and Communications (ICNC), Big Island, HI, USA, 2020, pp. 287-293, doi: 10.1109/ICNC47757.2020.9049732.



PACT

Partnership for Proactive Cybersecurity Research and Training

For more information please contact us at :

University of Arizona

Department of Electrical and Computer Engineering

1230 E. Speedway Blvd.
P.O. Box 210104
Tucson, AZ 85721-0104
www.nnsa-pact.org
info@nnsa-pact.org
Peter Kokabian
520-612-4645